

## REMARKS

This amendment responds to the Office Action mailed June 19, 2006. In the office action, the Examiner:

- allowed claims 1-6, 41 and 42;
- rejected claims 7-10, 12, 14-20, 22-23, 25, 27-33, 35-36, 38 and 40 as being unpatentable over U.S. Patent No. 5,912,947 to Langsenkamp et al. (Langsenkamp) in view of U.S. Patent No. 6,754,484 to Hiltunen et al. (Hiltunen) and further in view of U.S. Patent No. 6,798,867 to Zirngibl et al. (Zirngibl); and
- rejected claims 7, 12, 15, 25, 28 and 38 under 35 U.S.C. 103(a) as being unpatentable over Hiltunen in view of Zirngibl.

The pending claims are: claims 1-10, 12, 14-20, 22-23, 25, 27-33, 35-36, 38 and 40-42.

Langsenkamp discloses a public notification system, for notifying the public of relevant information about sex offenders, that minimizes the use of the notifying authority's, or caller's, personnel and communication lines. *See*, col. 2, line 57 – col. 3, line 10. As stated in the Office Action, in Langsenkamp **the caller does not specify a passcode, much less the claimed message-specific passcode specified by the first user**. In addition, as noted in the Interview Summary included with the Amendment After Final mailed March 10, 2006, the Examiner has agreed that the password in Langsenkamp is not message-specific, but “callee,” or recipient, specific. Nothing in the current Office Action disputes this agreed-upon interpretation of the scope of Langsenkamp.

Hiltunen discloses a short messaging system using information beacons in order to make transmission of a short message dependant on the intended recipient's location. *See*, column 1, line 41-57. The short messages can be “private” when only specified recipients are permitted access by using recipient specific encoding techniques. Furthermore, Hiltunen is concerned with minimizing memory usage at the beacon and so discloses that when a private message is delivered to the user it will no longer be available to the user. *See*, column 6, lines 29-33. Even for public messages or if delivery is unsuccessful, Hiltunen teaches setting a delivery time limitation after which the message is deleted from the beacon. No mention is made concerning redelivery of the message to the user. *See*, column 6, lines 33-42 and column 2, lines 5-26.

Regarding the requirement for associating a message-specific passcode with the voice organizer message, wherein the message-specific passcode is specified by the first user, the Office Action cites Hiltunen, column 4, lines 45-56 and column 5, line 51 through column 6 line 5. Here, Hiltunen discloses a preferred embodiment in which the message sender and the recipients must exchange “public keys” to identify themselves to each other. *See*, column 5, lines 21-28. Thus, a recipient must first specify a public key and transmit it to the message sender. Then, when the message sender wants to send a private message to the recipient, the sender uses the recipient’s pre-specified public key to encode the message. In another embodiment, Hiltunen discloses passwords corresponding to each recipient’s address. *See*, column 5, lines 29-32. The Office Action also cites Hiltunen, column 5, line 51 through column 6, line 5 and lines 29-37. This portion discloses the recipient of a private message entering an encryption password to gain access to the private message and the possibility of sending a reply to the originator and/or setting a time for deletion of private messages after the lapsing of a time delivery limitation. None of these features correspond to the claimed limitation of a message-specific passcode specified by the first user. Thus **the “public key” or password in Hiltunen is specified by the recipient, not the sender, and is not message specific, but instead is recipient specific.**

Zirngibl discloses a method and system of administering a dynamic voice-based service that can output information derived from an on-line analytical processing system to a subscribed user, including prompting the user for input and executing database queries in response to the user-entered input. Unlike, Langsenkamp, Hiltunen and the present invention, Zirngibl teaches a method of conducting real-time queries in response to real-time user inputs. The Examiner previously cited the PIN or personal identification number of Zirngibl as teaching the claimed message specific passcode, but since the PIN is neither message specific nor specified by the first user or creator of the message, the current Office Action correctly does not cite Zirngibl for claim limitations relating to the message-specific passcode. The Office Action does cite Zirngibl for periodically redelivering a voice message at a frequency specified by the first user wherein the frequency is selected from a group consisting of at least three frequencies. However, a close reading of the cited portions of Zirngibl shows that what is disclosed is scheduling conditions, including on a periodic basis, **for which the voice service is to be executed.** Since Zirngibl does not record and store a voice organizer message, as previously discussed in the Amendment mailed May 20, 2005, Zirngibl cannot redeliver such a message. Instead, based on a predetermined condition, the

voice service is executed or re-executed, but none of the disclosed voice services include periodically redelivering a recorded voice message.

1) Neither Langsenkamp, Hiltunen nor Zirngibl disclose a message-specific passcode.

Independent claims 7, 12, 15, 25, 28 and 38 recite, *inter alia*, “associating a message-specific passcode with the voice organizer message, wherein the passcode is specified by the first user.” As discussed above, neither Langsenkamp, Hiltunen nor Zirngibl teach a message-specific passcode, much less the first user of the system specifying the message-specific passcode to be associated with the voice organizer message. Instead, all of the cited art discloses recipient-specific passwords, PINs, and public keys. Hiltunen, while cited as meeting this claimed limitation, merely discloses that a message sender may receive a “public key” from a recipient and use it to encode a message for that particular recipient. As discussed more fully above, the teachings of Hiltunen do not meet the claimed limitation of a message-specific passcode specified by the first user. For at least the reasons explained above, claims 7, 12, 15, 25, 28 and 38 and their dependent claims are patentable over the combined teachings of Langsenkamp, Hiltunen and Zirngibl.

2) Neither Langsenkamp, Hiltunen nor Zirngibl disclose a message-specific passcode specified by the first user.

Independent claims 7, 12, 15, 25, 28 and 38 recite, *inter alia*, “associating a message-specific passcode with the voice organizer message, wherein the passcode is specified by the first user.” As discussed above, neither Hiltunen nor Zirngibl teach a message-specific passcode, much less the first user of the system specifying the message-specific passcode to be associated with the voice organizer message. For at least the reasons explained above, claims 7, 12, 15, 25, 28 and 38 are patentable over the combined teachings of Hiltunen and Zirngibl.

CONCLUSION

In light of the above amendments and remarks, the Applicant respectfully requests that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney at 650-843-7501, if a telephone call could help resolve any remaining items.

Date: September 19, 2006

Respectfully submitted,



Gary S. Williams

31,066

(Reg. No.)

**Morgan, Lewis & Bockius LLP**

2 Palo Alto Square

3000 El Camino Real, Suite 700

Palo Alto, California 94306

(650) 843-4000